facebook
twitter
newsbook.es

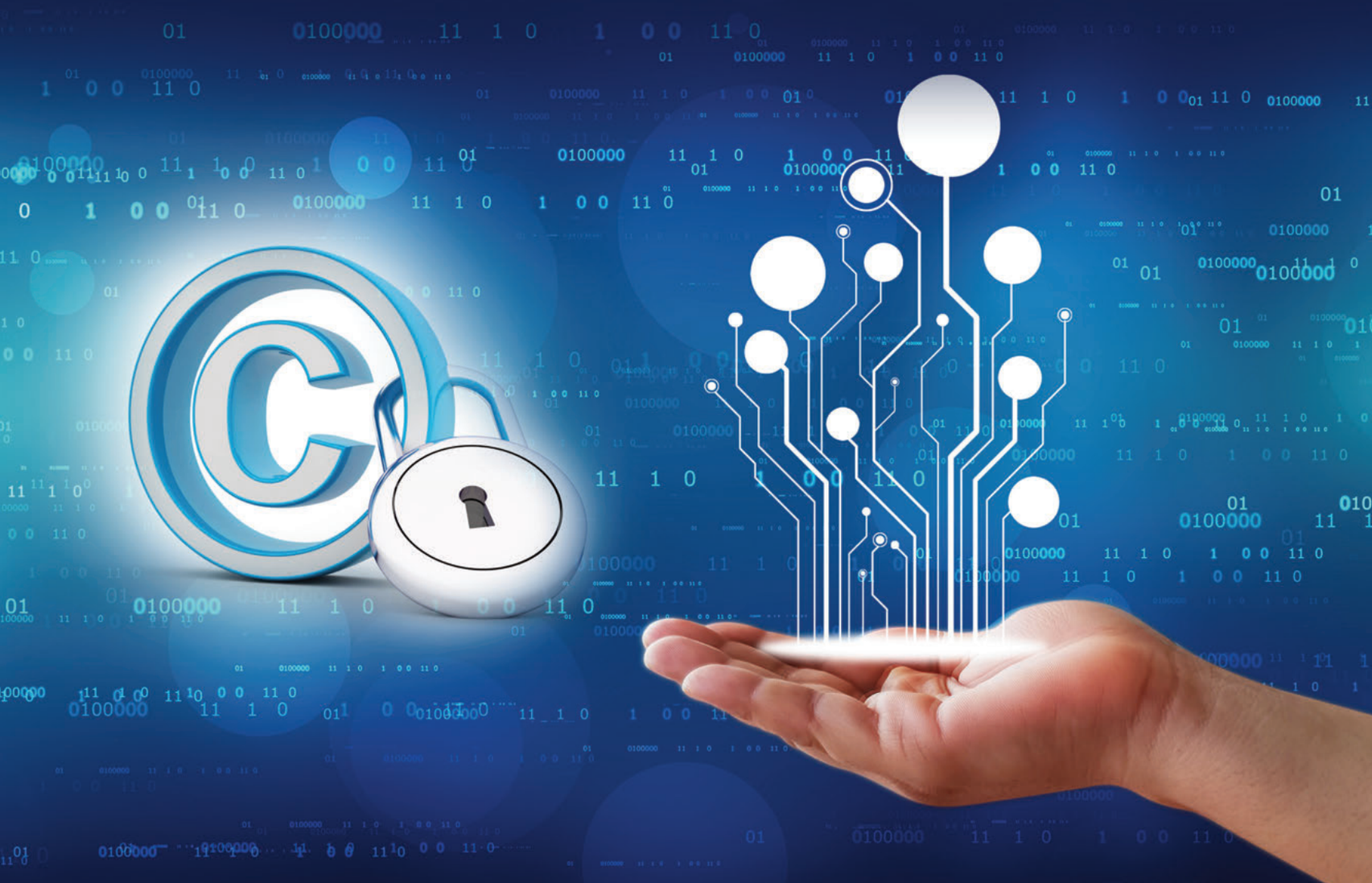
>> La revista del distribuidor informático

Newsbook

TAI editorial

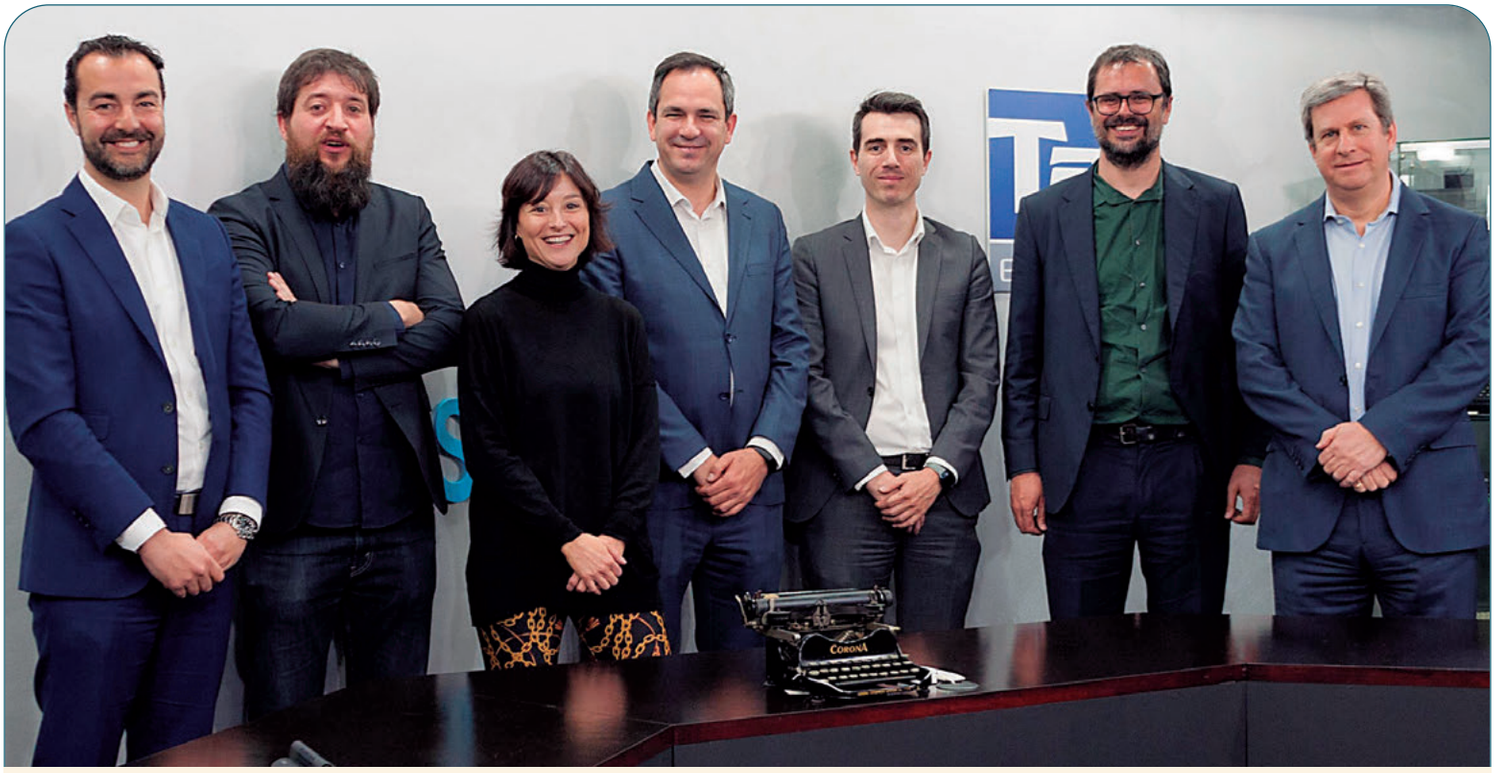
Año XXV Nº 259 Abril 2019 0,01 Euros

La seguridad exige que el canal mayorista trabaje su imagen de marca



La previsión es que en 2019 el mercado de la seguridad siga creciendo en España

Los mayoristas enarbolan la singularidad como valor para que el canal siga aprovechando la oportunidad de la seguridad



A pesar de estar ubicados en un segmento tan "privilegiado" en términos de rentabilidad y crecimiento como es la seguridad, los mayoristas reconocen que deben seguir innovando y adaptándose a las características de un mercado que exige estar siempre a la última. Las amenazas, cada vez más sofisticadas, no dejan de crecer y, con ellas, las necesidades de protección de las empresas. Un mercado, cada vez más complejo, que exige que cada empresa trabaje en su "imagen de marca". Una singularidad que los mayoristas construyen, sin olvidar la imprescindible oferta, en una propuesta de valor que comprende elementos como el soporte, la consultoría, la formación o la financiación. ¿El objetivo? Diferenciarse en un mercado cada vez más saturado para ser el mejor aliado del canal.

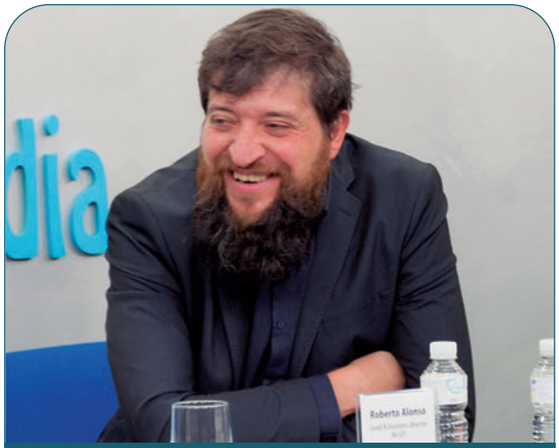
Marilés de Pedro

Echando un vistazo al mercado

Según calculó la consultora IDC, el pasado año el mercado de la seguridad creció en España entre el 8 y el 12 %. Un baremo, atractivo, que se espera repetir este año. "Cada vez hay más ataques y además son más sofisticados", recuerda Carmen Muñoz, directora general de Exclusive Group Iberia. Unos ataques que, a semejanza de los fabricantes (aunque con muy diferente objetivo), aprovechan las nuevas tecnologías, como es el caso de la inteligencia artificial, para perpetrar sus fechorías. "Permiten incluso automatizar la ciberdelincuencia".

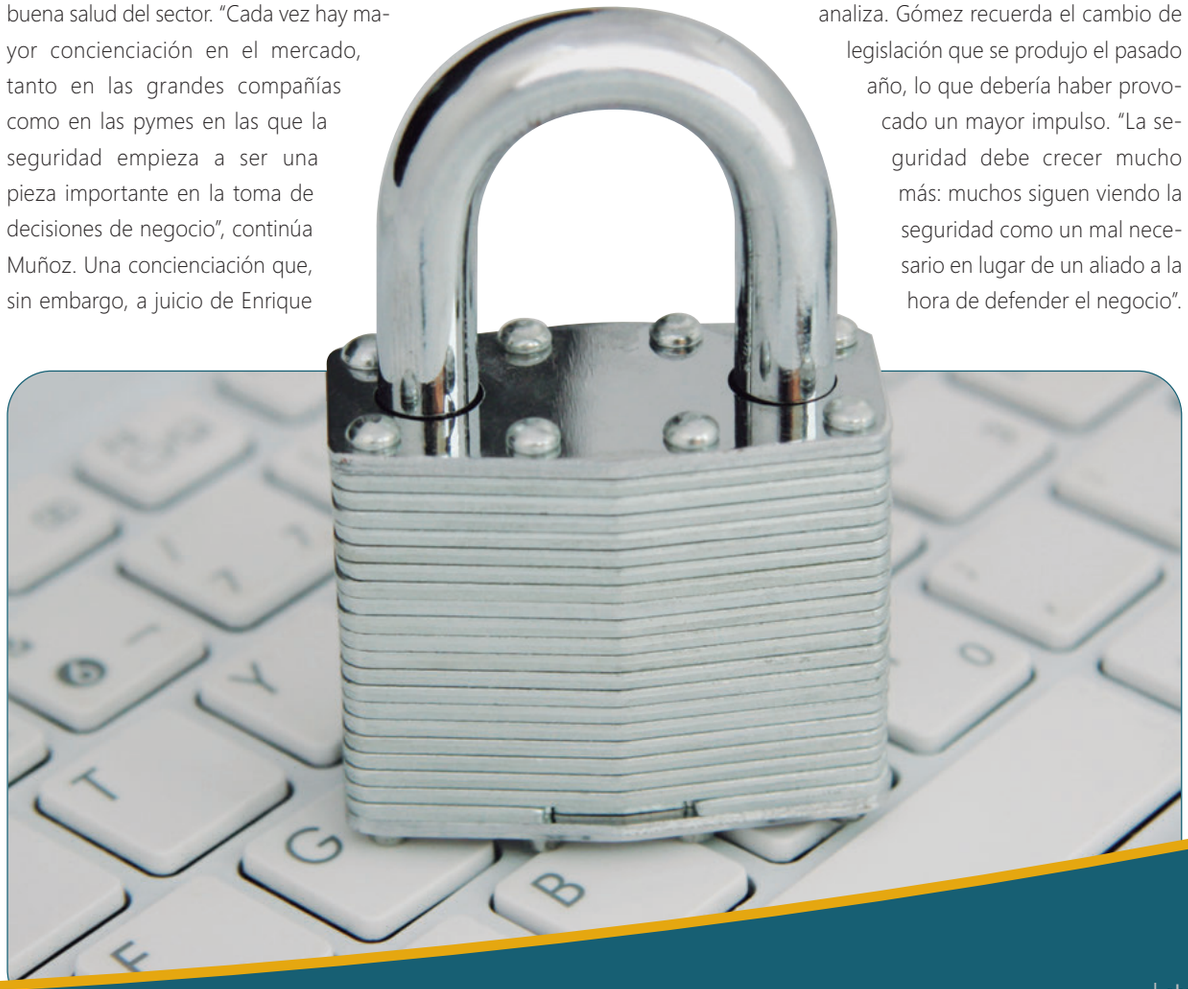
Aunque en 2018 no se produjeron ataques con una repercusión tan mediática como WannaCry, los ciberdelincuentes siguen lanzando amenazas, tanto generalizadas como inteligentemente dirigidas. No faltaron ataques tan destacados como el que afectó a Facebook, que provocó una enorme brecha de seguridad en la red social. De cualquier manera, las barreras son cada vez más poderosas. "Los fabricantes ya se han puesto a la altura adecuada para hacer frente a los ataques con tecnologías al alcance de todo el mundo", asegura Antonio Anchustegui, *business manager security* de la división Advanced Solutions de Ingram Micro.

Junto a este crecimiento del número de amenazas, el incremento de la concienciación contribuye a la buena salud del sector. "Cada vez hay mayor concienciación en el mercado, tanto en las grandes compañías como en las pymes en las que la seguridad empieza a ser una pieza importante en la toma de decisiones de negocio", continúa Muñoz. Una concienciación que, sin embargo, a juicio de Enrique Gómez, director de marketing de Aryan, aún no es suficiente. "Si existiera una verdadera concienciación, las cifras de crecimiento serían mucho más altas", analiza. Gómez recuerda el cambio de legislación que se produjo el pasado año, lo que debería haber provocado un mayor impulso. "La seguridad debe crecer mucho más: muchos siguen viendo la seguridad como un mal necesario en lugar de un aliado a la hora de defender el negocio".



Roberto Alonso,
cloud & business director de **GTI**

"Es mucho más interesante vender seguridad que pura infraestructura"



Lista de amenazas

En España, según calcula INCIBE, el pasado año se incrementó el número de incidentes de ciberseguridad de 18.000 a 123.000 con tres tendencias en cabeza: el *ransomware*, el uso del *malware* para ganar persistencia y el fraude conseguido gracias a las técnicas de fraude.

En esta lista de amenazas siguen permaneciendo los "imprescindibles": el *ransomware*, el *phishing*, los ataques de denegación de servicio, etc. Ahora bien, a la cabeza de las prioridades de las empresas de seguridad está la protección del dato. "Es lo que persiguen los maleantes", recuerda Iñaki López, *regional manager* de Arrow en España y Portugal. "Las empresas, incluidas las pymes, están cada vez más concienciadas de esta protección". Una concienciación que alcanza, sobre manera, al entorno del puesto de trabajo que como asegura López es donde más información se aloja. "Y, sin embargo, es el área en el que menos están invirtiendo las empresas".

Una protección que, como recuerda Jorge Puerta, director comercial de Ingecom, incluye su cifrado y una autenticación fuerte. "Hay que estar protegido contra la fuga de información, lo que obliga a contar a las empresas con herramientas de DLP, por ejemplo".

El control y la gestión de los empleados señala otro área de alerta. "El empleado sigue siendo el eslabón más débil de la cadena", recuerda la máxima responsable de Exclusive Group Iberia. "Todo lo que tiene que ver con comportamiento del usuario es clave; lo que se constituye en una de las brechas principales que tienen las compañías; no tanto el perímetro".

Otra amenaza cada vez más extendida es el *phishing* que hace uso de las cuentas del CEO o del director general. "Es relativamente novedoso y muy dañino", recuerda Antonio Anchustegui. El método es "sencillo" y hace uso de técnicas de ingeniería social: un empleado de alto rango o con capacidad para hacer transferencias y que tiene acceso a da-

Las amenazas que no cesan…

A pesar de la irrupción de nuevas fórmulas maleantes, el *ransomware* sigue siendo una de las amenazas más virulentas. Un tipo de ataque que "democratizó" las amenazas: su carácter generalista, que permite atacar a cualquiera, extendió el ámbito de actuación de los maleantes.

A lo largo del pasado año, sin embargo, se observó un aumento en el número de ataques de *ransomware* dirigidos y más sofisticados. A pesar de que su número es menor que los ataques masivos que fueron la tónica dominante en 2017 son, sin duda, mucho más peligrosos. Algunos de estos ataques, como fue el caso de SamSam o Dharma, tuvieron una enorme popularidad por el impacto económico que cosecharon.

El *ransomware* ha sufrido una rápida transformación en los últimos tres años, mejorando la arquitectura del *malware* para aumentar su precisión y las técnicas para acceder a las *botnets*. También ha cambiado el objetivo de sus campañas, con capacidad para cifrar los recursos de las redes corporativas, multiplicando así su poder y alcance. Y todo ello sin olvidar la precisión en los ataques más sofisticados y masivos, en los que varios archivos se infectan de manera simultánea.

Los ataques, además, están cada vez más ocultos pero son terriblemente efectivos. Se ha pasado de los ataques más tradicionales vinculados con el *phishing*, el robo de cuentas, credenciales, etc. a ataques basados en *malware* sin ficheros; que aprovechan el uso de tecnologías totalmente permitidas, para introducir pequeñas piezas para causar el ataque. Una técnica que es mucho más complicada de detectar ya que no cuenta con piezas evidentes de *malware*.

El área de la inteligencia artificial, que ha permitido tantos avances en las técnicas de protección, también es accesible para "perfeccionar" los ataques. Es una consecuencia de la democratización de las herramientas, a las que acceden también los cibercriminales.

Tampoco hay que olvidar todo el volumen de datos, con la enorme dispersión existente debido a las múltiples fuentes de las que proceden, que permiten realizar a los ciberdelincuentes de manera precisa un perfil para acceder a los datos más personales.

Una de las tendencias maleantes que se ha consolidado es el minado de criptomonedas. Se trata de una técnica que roba los recursos de cómputo de los equipos y que es complicado de detectar por parte de los usuarios. Incluso ya está empezando a afectar a los teléfonos móviles: se roba la capacidad de la batería, lo que ralentiza el uso de las aplicaciones.

La pérdida de datos y la fuga de la información son otro grave quebradero de cabeza para las empresas. Se ha observado un aumento de la presencia de aplicaciones troyanas en Google Play y Apple App Store, capaces de robar credenciales de los usuarios e interceptar mensajes de texto, así como introducir criptomineros ocultos ayudándose de aplicaciones supuestamente inofensivas.

Los dispositivos conectados siguen siendo un objetivo muy apetecible y será, sin duda, uno de los entornos que más serán atacados en los próximos años. Más teniendo en cuenta que muchos de ellos no cuentan con la protección adecuada.

La lista, que podría ser interminable, también incluye al "tradicional" *phishing* que afectó a marcas y compañías muy conocidas en España, o los ataques a los bancos. Sin olvidar, el gran reto que abre el desarrollo del IoT. Una gran parte de los sistemas que forman parte del IoT e, incluso, del OT en sí, tienen, por defecto, una seguridad débil. La mayoría viene con unos parámetros de fábrica que normalmente no se cambian e integra un *firmware* que es muy complicado de actualizar; lo que complica sobre manera la protección.

arrowecs.es

Leading **Security Solutions** distributor

Cybersecurity is essential in today's environment of hackers, malware, viruses, spyware and more.

Establishing a complete, *end-to-end* cyber security framework is critical to ensuring a **comprehensive, efficient, compliant and secure enterprise**.

Five Years Out

algosec · allot (See. Control. Secure.) · ARISTA · aruba (a Hewlett Packard Enterprise company) · Carbon Black. · Check Point (Software Technologies Ltd.)

f5 · FireEye (Security Reimagined) · FORTINET · gemalto (security to be free) · HUAWEI · IBM (Business Partner)

Infoblox (Control Your Network) · ixia (A Keysight Business) · MICRO FOCUS · NETSCOUT · Pulse Secure · radware (Every second counts)

splunk> · swivelsecure · Symantec · tenable · TREND MICRO · viewtinet

ARROW ECS • Avenida de Europa, 21 Parque Empresarial La Moraleja • 28108 Alcobendas, Madrid
Tel. + 34 91 746 02 20 • marketing.ecs.es@arrow.com

tos de cuentas, recibe un correo, supuestamente de su jefe, ya sea su CEO, presidente o director de la empresa; donde se le solicita que lleve a cabo una operación financiera.

Enrique Gómez alerta de que no existe ninguna tecnología de seguridad capaz de actuar, de manera completamente efectiva, contra la ingeniería social. "Cualquier usuario, con su comportamiento, puede ser una fuente de amenaza. Los ataques que van directamente contra el usuario son los más peligrosos". En su opinión, si se mide la "rentabilidad" que consiguen los maleantes, la "estrella" sigue siendo el *ransomware*, "Se trata de un ataque con múltiples trampas ya que además del bloqueo del dato, si el usuario decide abonar el rescate, entra en una dinámica de la que es complicado salir ya que los ciberdelincuentes lo señalan como una víctima recurrente".

Ante toda esta batería de ataques, Roberto Alonso, *cloud & business director* de GTI, recuerda que en la actualidad se trabaja de forma intensiva en la prevención. "Y en el caso de que el ataque tenga lugar, en una respuesta rápida ante lo que ha sucedido".

Sin embargo, a pesar de este amenazador panorama, hay muchas empresas que todavía no se han dado cuenta de que tienen que invertir en seguridad. Así lo cree Chuck Cohen, fundador y director general de Ireo. "Hay otras que invierten sin tener un plan de seguridad definido", completa. En su opinión, las soluciones de seguridad deben ser manejables con los recursos que tienen las empresas. "No todo el mundo puede administrar los sistemas complejos que se están lanzando al mercado; sobre todo en el segmento medio en el que los recursos son limitados y poco especializados en la seguridad. Es una lucha por maximizar la seguridad manteniendo una facilidad en el uso de la misma".

Enrique Gómez,
director de marketing de **Aryan**

"La seguridad debe crecer mucho más: muchos la siguen viendo como un mal necesario en lugar de un aliado a la hora de defender el negocio"

amenazas que tienen como objetivo este entorno y, por ende, las tecnologías que se utilizan para detenerlas, han dado un empuje a este entorno, con soluciones que van mucho más allá del antivirus". Puerta insiste en que es este ámbito el que aglutina una gran parte de la gestión de los datos, lo que le confiere una gran criticidad. "El peligro no solo viene de fuera, también de dentro: de la gestión del dato por parte del usuario", insiste.

Una creciente importancia que ha permitido que este entorno exhiba una personalidad de "navaja suiza", como lo ha bautizado Anchustegui donde convergen las soluciones de DLP, cifrado, EDR, EDP *(Endpoint Detection and Protection)* o módulos de *machine learning*, entre otras. "Antes era un entorno que muchas marcas despreciaban y ahora es estratégico". Una situación que ha permitido que si antes se desdeñaban operaciones de cambio de un proveedor a otro en este entorno "porque podían ser una fuente de problemas",

Según calculó la consultora IDC, el pasado año el mercado de la seguridad creció en España entre el 8 y el 12 %

La resurrección del *endpoint*

En los últimos tiempos, la mayor parte de las compañías de seguridad, que habían centrado sus esfuerzos en otros apartados, han vuelto sus ojos hacia el puesto de trabajo que se ha convertido en una enorme puerta de entrada a los "nuevos" ataques. Se trata de una resurrección de este entorno que, según calcula IDC, atesorará el 18 % de la inversión que se realice en el ámbito de la seguridad en España en 2019. "Es un negocio que ha crecido mucho, empujado por el *ransomware* y por la oferta de productos vinculados con EDR *(Endpoint Detection and Response)*", explica Jorge Puerta. "El clásico negocio del antivirus estaba oxidado; pero las

La especialización es la clave

En un mercado más o menos maduro como el de la ciberseguridad, dónde los fabricantes tradicionales de cortafuegos quieren ampliar su mercado y están tratando de llegar al endpoint; y los que se mueven en el endpoint quieren proteger otros ámbitos como CASB, nuestra estrategia se basa en aportar conocimiento para evitar los silos aislados. La seguridad aislada no tiene sentido. Hay que apostar por distintas soluciones que traten de proporcionar una protección lo más completa posible, facilitando la reducción de la superficie de ataque de las organizaciones. Nuestra clave ha sido la especialización y la formación de un equipo adecuado con experiencia y conocimiento del mercado.

Las certificaciones de los fabricantes de seguridad generalmente están asociadas a tecnologías más consolidadas por lo que hemos preparado para nuestros *partners* formaciones no oficiales complementarias que enseñen a proteger aspectos menos tradicionales de la seguridad. Queremos convertirnos en su socio, ayudarles a adentrarse en áreas más específicas y disruptivas en el mercado de la seguridad como la visualización de tráfico este-oeste, las soluciones CDN y WAF, las tecnologías para combatir amenazas avanzadas... A día de hoy no aparecen tantos proyectos de tecnologías complementarias para que los canales de seguridad se especialicen, por eso, desde V-Valley les ofrecemos todo el apoyo necesario, conjuntamente con los fabricantes.

Alberto López,
Director del área de seguridad de ***V-Valley***

Conforme las tecnologías se van popularizando y la tecnología se va estandarizando, recomendamos a nuestros clientes que busquen tecnologías menos implementadas y que, por ejemplo, investiguen dentro de las redes de sus clientes para averiguar qué dispositivos tienen tanto en IT como en OT, y así puedan proporcionar servicios de descubrimiento tecnológico que no cobramos al canal, pero que ellos sí deberían cobrar a sus clientes. Nuestro trabajo con el *partner* es ofrecer un servicio de asesoría para obtener buenos réditos con sus clientes.

Hoy en día, con los métodos tradicionales de tecnologías de seguridad, resulta imposible llegar a dar respuesta a las amenazas tan constantes y complejas que se están produciendo. Para poder hacer frente a esta situación, resulta vital la automatización de los procesos y emplear consolas SIEM para visionar todo el tráfico. No todas las empresas necesitan un servicio 24x7, ni visualización o informes, pero teniendo en cuenta las necesidades de sus clientes, cualquier *partner* puede ofrecer este tipo de servicios, con mayor o menor complejidad, a sus clientes.

Por poner un ejemplo de nuevas oportunidades, Microsoft, a través de Azure, protege las comunicaciones e infraestructuras propias de su nube, pero no los datos de las empresas que están alojados. Observamos con preocupación que las organizaciones, o no están implementando soluciones de seguridad en Azure, teniendo los datos en la nube, o si lo hacen, es con soluciones de seguridad muy básicas propias de la arquitectura Azure que se limitan a IPS o a un *firewall* para realizar protección de capa 2 y 3. Estamos volviendo a la protección tradicional. Hemos de ser conscientes de que ahí arriba estamos desprotegidos; por lo que se abre una gran oportunidad de negocio.

"La seguridad aislada no tiene sentido. Hay que apostar por distintas soluciones que traten de proporcionar una protección lo más completa posible"

Carmen Muñoz,
directora general de **Exclusive Group** Iberia

"Exclusive es el mayorista de las *startups* por excelencia. Nos fijamos en su capacidad de innovación y en su adecuación a las necesidades del mercado"

ahora, "al desaparecer el perímetro, vuelven a cobrar importancia", asegura Roberto Alonso. "Es primordial observar cómo se comporta el usuario y detectarlo de otra manera". A pesar de esta resurrección, aún queda mucho camino por recorrer. "No es una prioridad", cree Iñaki López que recuerda que, según un estudio reciente, el 32 % de las compañías coloca el *endpoint* en segundo lugar en su ranking de inversión. "Falta proteger el dispositivo, más si se trata de uno personal. Queda mucho por concienciar qué se protege y cómo".

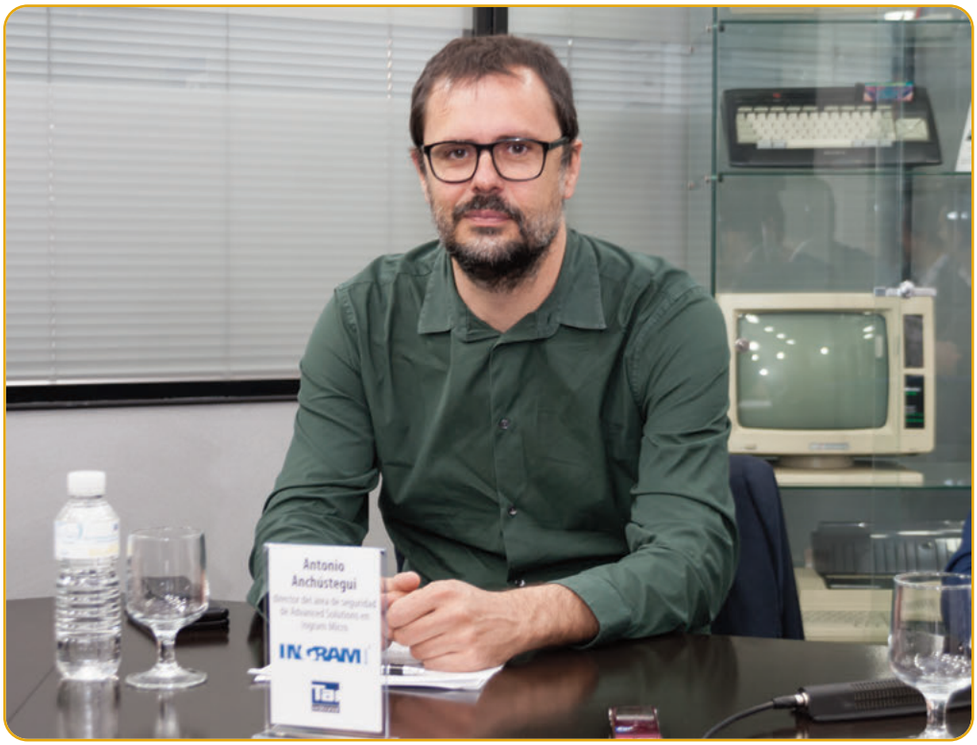
¿Quién se llevará el gato al agua en el *endpoint*?

Prueba de esta resurrección es el enorme número de marcas que compiten en este apartado. Junto a los fabricantes tradicionales que estaban focalizados en el entorno de red y que ya cuentan con soluciones específicas para el puesto de trabajo, lo que les permite contar con una plataforma completa de seguridad y ofrecer a los clientes la posibilidad de una gestión unificada de ambos entornos; se han posicionado innovadoras marcas con un foco exclusivo en este área. "Es un área de prioridad para el canal y para las marcas", resume Carmen Muñoz. Ahora bien, ¿quién se llevará el gato al agua en el mercado?

Chuck Cohen recuerda, con plena razón, que las grandes marcas exhiben la ventaja de su fortaleza financiera. "Pueden sacar el talonario y comprar, lo que les permite ampliar su oferta de manera más rápida". Junto a esta mayor capacidad de recursos, pueden abarcar mayor área de protección, lo que les permite gestionar, de manera más centralizada, la seguridad de las empresas. Apostar por las *startups* no es sencillo pero muchos de los mayoristas que trabajan en España han apostado (y apuestan) por ellas. Cohen prevé, sin embargo, que la mayoría de ellas no permanece en el mercado muchos años. "Bien porque fracasan, bien porque son compradas por compañías más grandes", asegura.

La revolución del puesto

En relación a la seguridad IT, siempre hay opiniones para todos los gustos. Nosotros somos optimistas y pensamos que últimamente los buenos están ganando la partida y que los malos lo tienen más difícil que hace unos meses.



Antonio Anchustegui
*Ebusiness manager security de la división Advanced Solutions de **Ingram Micro***

Los fabricantes están haciendo un buen trabajo, poniendo a disposición del mercado tecnologías utilísimas e integradas, a precios asequibles, que hace poco tiempo eran mucho más exclusivas. En particular el puesto de trabajo ha evolucionado enormemente y presentamos interesantes novedades en este área.

"Los fabricantes están haciendo un buen trabajo, poniendo a disposición del mercado tecnologías utilísimas e integradas, a precios asequibles, que hace poco tiempo eran mucho más exclusivas"

Ramillete de fabricantes en Ingram Micro

- SonicWall Capture Client incluye protección avanzada y permite la visibilidad y el análisis del tráfico encriptado. Incorpora visualización en tiempo real de amenazas y seguimiento de *malware* EDR, pudiendo hacer *roll-back* al estado previo a la infección. Ofrece además informes muy fáciles de usar.
- Sophos ofrece una solución para el puesto de trabajo muy versátil, pudiendo combinar su motor tradicional y el avanzado Intercept X, ahora con EDR. Es una de las tecnologías más reconocidas del mercado en este entorno. Combina el *deep learning* con la mejor tecnología *antiexploits*, la tecnología *antiransomware* CryptoGuard y el análisis de causa raíz. EDR le pone la guinda a una *suite* completísima de protección del puesto y su seguridad sincronizada alerta de la amenaza a todos los puntos Sophos de la red, tanto en el entorno del puesto como en el perímetro.
- Symantec cuenta con su Endpoint Protection 15, que incluye gestión completa en la nube y herramientas *antimalware*, *advanced protection*, *detection*, prevención de *exploits*, *application isolation* y control y EDR. Como una navaja suiza, el agente permite el despliegue de proyectos de *proxy* en la nube / Web Security Services, DLP, CASB o cifrado, con un enfoque análogo al que tenían tradicionalmente los NGFWs, en este caso en el puesto.
- Por último, y no menos importante, Symantec y Sophos tienen *suites* completas de protección de dispositivos móviles que, debido a la menor implantación de medidas correctoras, son ahora un vector prioritario de ataque por parte de los creadores de *malware*.

Iñaki López,
regional manager de **Arrow** en España y Portugal

"Hay que trabajar más para nuestra propia marca y construir soluciones que nos hagan únicos"

Carmen Muñoz, fiel a la filosofía que ha marcado el paso del mayorista que dirige, defiende la apuesta por las *startups*. "Somos el mayorista de las *startups* por excelencia". La directiva explica que los factores que guían la selección son tecnológicos. "Nos fijamos en su capacidad de innovación y en su adecuación a las necesidades del mercado". El modelo de *go to market* es fundamental. "He visto soluciones que en España funcionan muy bien y que, sin embargo, no ha sido así en otros mercados. Depende de la estrategia en cada mercado y el comportamiento de los clientes. Hay mercados en los que los clientes son mucho más innovadores y no les da miedo implantar una solución de una de estas compañías; y otros más conservadores que prefieren dejar su protección en manos de marcas más tradicionales de las que ya tienen soluciones en otras áreas del perímetro".

Apostar por ellas también tiene riesgos. "Solo algunas tienen un éxito sostenible", recuerda Jorge Puerta. "Y si triunfan, muchas veces son compradas por una grande". Un panorama que no cambia el papel que le toca jugar a un mayorista de valor. "Nos corresponde aportar ese valor al mercado e investigar qué tecnologías atractivas aparecen, adquirirlas y lograr una capilaridad adecuada en el mercado. Se trata de ayudar al canal a llevarlas al mercado".

Quizás la convivencia sea posible. "El papel de las *startup* es estratégico para cubrir novedades, siendo más disruptivas a nivel tecnológico que las grandes", recuerda Iñaki López. "Es innegable que cuantas más soluciones tenga un fabricante en su catálogo, que le permitan proteger el *cloud*, el *endpoint* o el perímetro, su ventaja será mayor".

El empuje de las grandes es innegable. Roberto Alonso recuerda las grandes inversiones que están haciendo las compañías tradicionales del segmento de la seguridad para proteger, de manera adecuada, este entorno. "Son fabricantes muy potentes, con una enorme base instalada, lo que les permite disfrutar de una ventajosa posición".

Y la red... Que no pierde comba

El incremento de las inversiones en torno a la seguridad del puesto de trabajo no hace olvidar el tradicional entorno de red. A este apartado calcula IDC que se destinará el 14 % de las inversiones en España. "Es lo más obvio ya que era el área en el que primero se colocaba la protección", recuerda Chuck Cohen. "Lo que se olvida es que por muy buena que sea la puerta, si no se cuida la ventana seguiremos siendo vulnerables", alerta. "Hoy en día ya no está claro el perímetro".

Según INCIBE, en 2018 se incrementó el número de incidentes de ciberseguridad de 18.000 a 123.000 con tres tendencias en cabeza: el *ransomware*, el uso del *malware* para ganar persistencia y el fraude conseguido gracias a las técnicas de fraude

Existe, como recuerda Roberto Alonso, una mayor preocupación para conseguir que todas las capas se hablen. "Lo que permite implantar una mejor política de prevención". Esta rotura del perímetro ha permitido que el área industrial converja con el entorno tradicional TI. Cada vez se observa una mayor inversión es el entorno industrial, uno de los segmentos que más importancia tendrá con la explosión del IoT.

SOLUCIONES DIFERENCIALES PARA SEGURIDAD IT

25 ANIVERSARIO Aryan
VALUE ADDED IT SOLUTIONS

Back Up | Wifi Seguro | Seguridad Empresarial | Seguridad Perimetral
Seguridad EndPoint | TDR | Multifactor Authentication
Data Loss Prevention | Protección del Datacenter

25 Años haciendo negocios juntos

¿HABLAMOS? 902 386 902

www.aryan.es

25 ANIVERSARIO Aryan SEGURIDAD IT

WatchGuard HUAWEI ctera Bitdefender F-Secure COSOSYS

Madrid: 916 574 848 | Barcelona: 933 636 320 | Valencia: 963 467 245

El eterno reto de los servicios gestionados

Los servicios gestionados marcan el futuro de la seguridad. Asegura IDC que el 25 % de la inversión en materia de seguridad irá a este apartado en España en 2019. "Es un mercado en crecimiento en el que tenemos que hacer nuestro trabajo habitual de formar, introducir las mejores tecnologías y sobre todo proporcionar una capa de financiación ya que, a pesar de que hay muchas marcas con capacidad de desarrollo en este apartado, no tienen un modelo de negocio para aprovecharlo", recuerda Iñaki López.

Los mayoristas cuentan con plataformas propias que permiten al canal aprovisionar esas tecnologías y gestionar esos servicios. Una parte muy importante de estos servicios gestionados se convierte en margen para el canal. Como recuerda Chuck Cohen, el negocio que obtiene el mayorista con este modelo no es muy grande. "Nuestro valor añadido es proporcionar la plataforma y el margen lo gana el canal. No representa nuestro negocio más rentable; pero el canal que no reconozca esta gran oportunidad no tiene mucho futuro".

La pyme parece ser el mercado natural de estos servicios gestionados. "A medida que la pyme sea más consciente, es una oportunidad de negocio muy grande para el canal", apunta Carmen Muñoz. "La pyme es el apartado en el que más dificultad hay para adoptar soluciones de seguridad y este modelo que ofrecen los socios es perfecto para este tipo de empresas. Permite a la pyme invertir de acuerdo a su tamaño y a su capacidad".

Ya hay distribuidores que están ofreciendo servicios de esta índole sin cobrar por ello. Antonio Anchustegui asegura que en el ámbito de la pyme es donde más se utiliza este tipo de servicios. "Ahora bien, de manera informal y gratuita", especifica. "Hay que poner en valor esa labor del canal: el distribuidor debe ofrecer informes, actualizar las políticas de seguridad de sus clientes, etc.".

A pesar de que los modelos de pago por uso están asentándose en un enorme abanico de áreas tecnológicas, "en el área de la seguridad todavía queda mucho por hacer", resume Roberto Alonso. "No es fácil para un distribuidor adaptar su negocio a este modelo de venta y tampoco es sencillo buscar la tecnología adecuada", continúa. "Hay que recordar que es un modelo que tarda más en arrancar ya que implantar y desarrollar un servicio gestionado requiere un tiempo mayor que cualquier otro modelo".

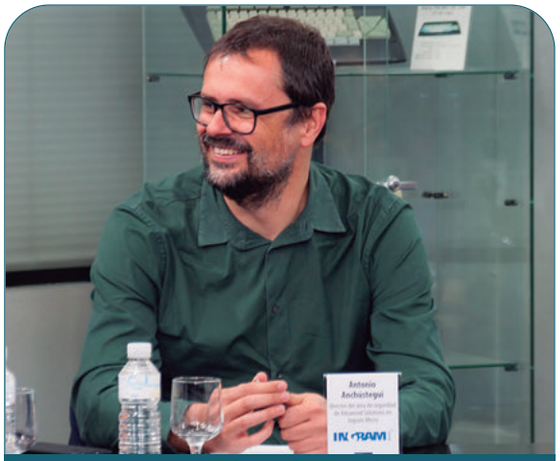
Pero marca el futuro. "La tendencia es convertirlo todo en servicio y que el canal mayorista sea pieza importante del mismo", prevé Jorge Puerta. Un negocio que exige formación y… recurrencia. "Es el modelo que va a crecer gracias a su carácter recurrente", apunta Enrique Gómez. "El canal necesita un conocimiento y una formación específica para adaptarse a las nuevas exigencias de este modelo".

Seguridad y nube, el matrimonio que funciona

El matrimonio entre la seguridad y la nube sigue proporcionando destacados vástagos. "La nube está permitiendo, gracias al discurso que están pronunciando algunas marcas, que aumente la concienciación sobre la seguridad", asegura Roberto Alonso. GTI ha llevado a cabo una profunda transformación de su modelo de negocio para apuntar únicamente a este entorno. "Cada vez hay más proyectos, incluso en empresas más pequeñas, en torno a ella", asegura. Ahora bien, reconoce que la seguridad, sobre todo en las empresas más grandes, tiene un papel crítico en el desarrollo de los proyectos en la nube. De lo que no tiene duda es de que es "mucho más interesante vender seguridad que pura infraestructura".

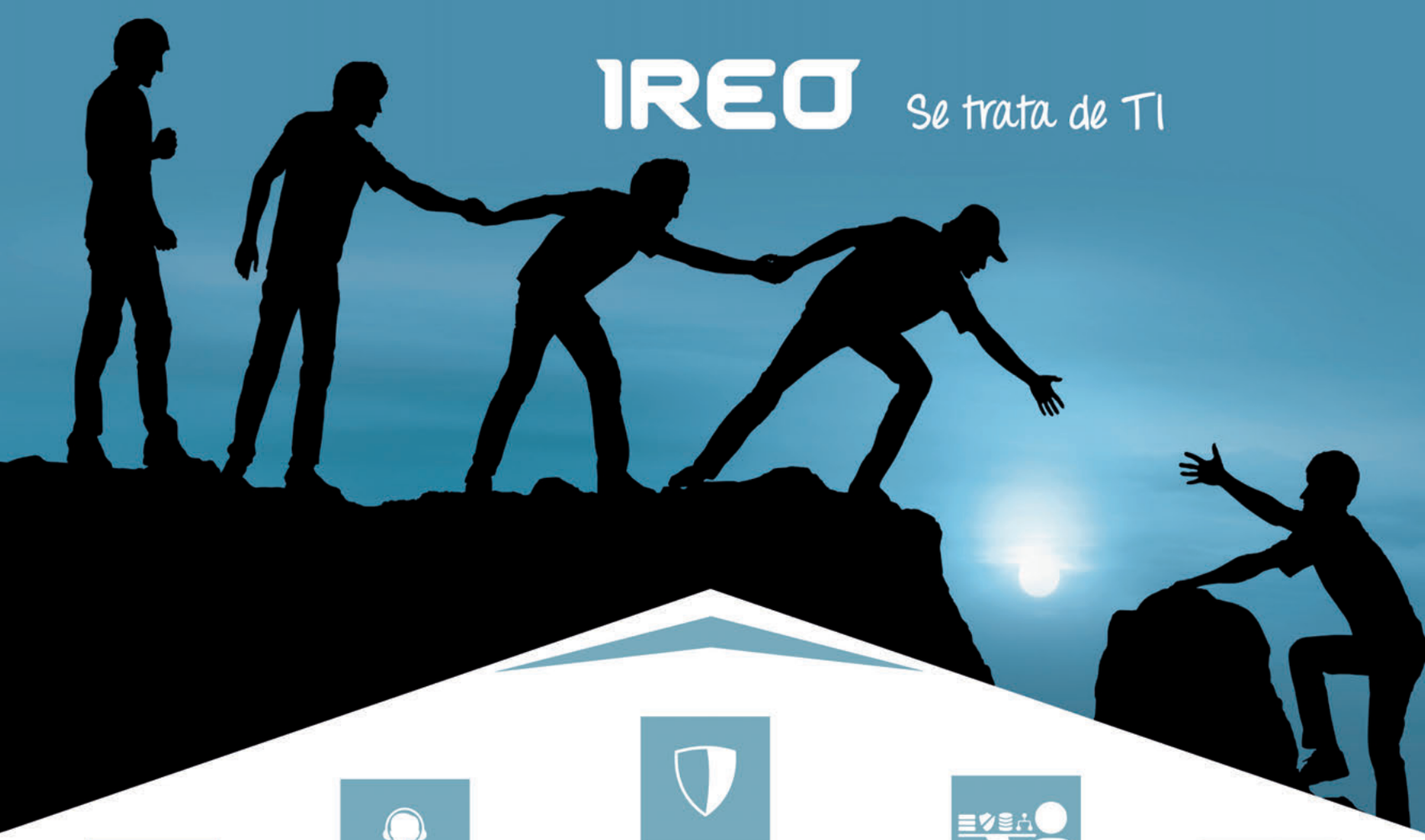
Iñaki López recuerda que hay dos "entornos" distintos que observar. "Hay que proteger la *cloud* en cualquiera de sus formatos; público, privado o híbrido; un entorno en el que el papel de las marcas es vital para desarrollar las soluciones adecuadas". Y por otro lado, la nube como modelo de negocio para la seguridad que permite al cliente hacer provisión de servicios y soluciones de seguridad desde la nube. "Es aquí donde el canal debe desarrollar su papel".

El panorama de la nube es absolutamente heterogéneo: añade complejidad a la gestión pero también abre numerosas oportunidades. "La clave reside en los mayoristas y en el



Antonio Anchustegui,
business manager security de la división Advanced Solution de **Ingram Micro**

"Los fabricantes ya se han puesto a la altura adecuada para hacer frente a los ataques con tecnologías al alcance de todo el mundo"



SISTEMAS

ITSM

SEGURIDAD

MSP

NETWORKING

BeyondTrust

cherwell

DataLocker
Simply Secure

datto

deepnet
Security

Endpoint Protector

Ericom
Be Connected, Be Secure

Kanguru
Secure. Anytime. Anywhere.

KEMP

macmon
nac smartly simple

ManageEngine

Prot-On
Protect what you share

SCALE
COMPUTING

SKYBOX
SECURITY

SOPHOS

StorageCraft

STORMSHIELD

TITUS

Trustwave

IREO

Castrobarto, 10 - 4ª Planta | 28042 Madrid | España | Tel.: 91 312 13 86 | info@ireo.com | **www.ireo.com**

canal a la hora de ayudar a prescribir y a dar consultoría a las empresas que están yendo al *cloud* por decisión de negocio", argumenta Carmen Muñoz. "La seguridad es un reto en este entorno *cloud*; cuánto más heterogéneo es el panorama, más riesgos hay. Y, por tanto, más oportunidades".

Al canal le queda mucho por aprender en este entorno de la nube. "Le queda mucho por conocer los nuevos entornos relacionados con la nube (Azure, Google, etc.)", explica Antonio Anchustegui. "Deben entender cómo funcionan y deben observar cuál es su papel en este entorno: Microsoft está haciendo mucho desarrollo de las soluciones de seguridad. Quiere ampliar su presencia mucho más allá de la infraestructura", alerta.

La oportunidad procede, como no podía ser de otra manera, del valor. "Debe saber aprovecharla", insiste el director general de Ireo. En el caso de uno de los productos estrella de Microsoft, Office365, recuerda que muchas compañías aun no tienen claro que su venta exige el complemento de soluciones de *backup*, de filtrado de correo electrónico o de herramientas de administración. "Se piensa que se trata de un producto completo, cuando no es así", insiste. "Lo que abre muchas oportunidades al canal".

Queda mucho camino por recorrer. "El mensaje de *cloud* es una realidad pero en el tema de la seguridad hay mucho por delante", asegura el director comercial de Ingecom. También en el canal. "Más que el fabricante, debe ser el distribuidor el que se convierta en prescriptor y el que otorga confianza", apunta Enrique Gómez. "Es la compañía capaz de mover de una a otra tecnología al cliente". Sin embargo, falta que el canal "tenga más claro cuál es su papel y su negocio".

¿Tiene fecha de caducidad el crecimiento del mercado?

La seguridad es uno de los apartados con más tradición en el canal mayorista. A pesar de su crecimiento y de su buena salud, a semejanza de lo que ha sucedido en otros segmentos, los márgenes se han estrechado y aseguran muchos distribuidores que cada vez es más complicado cerrar los proyectos. ¿Tendrá fecha de caducidad el crecimiento de este mercado? A juicio de Iñaki López, la respuesta es negativa. "Es un mercado que está evolucionando", puntualiza.

De idéntica opinión es Roberto Alonso. "Seguirá creciendo", corrobora. "Es cierto que los márgenes están cayendo pero el mercado se va a mantener. Lo que se está transformando es la manera de vender y aprovisionar".

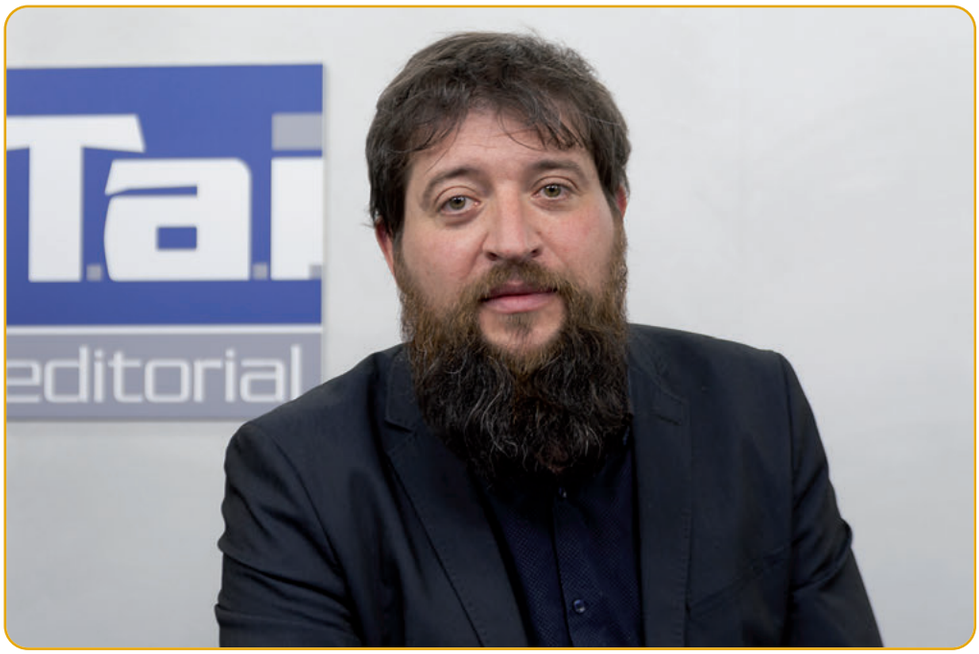
Al rebufo de los buenos crecimientos que ha tenido este mercado en los últimos años ha aumentado el número de compañías que ha decidido apostar por él. De ahí la caída en los márgenes. "Hay tanta competencia que va a llegar un momento en el que nos canibalizaremos unos a otros", alerta Jorge Puerta. "Se trata de un mercado, constituido por marcas y compañías de canal, que crece más que la demanda; lo que conducirá a una ralentización del crecimiento".

Algunos observan esta caída de márgenes si el canal solo se centra en algunos mercados más maduros y tradicionales. "Si es un distribuidor que ha apostado por la nube o los servicios gestionados; que son las vías de desarrollo futuro; el margen es mucho mayor", recuerda Iñaki López.

La venta del dispositivo, sin más, hace mucho tiempo que caducó. "Es un mercado que exige un modelo continuo de cambio", explica Carmen Muñoz, que puntualiza que las pri-

Cuando la información crítica de una empresa reside en un portátil

El mercado de la seguridad ahora llamado ciberseguridad, que seguramente es la evolución a un nombre más poderoso y/o amenazante, es un mercado en constante crecimiento, de igual manera que son crecientes las amenazas o los ciberataques. Las predicciones también siguen una tendencia ascendente en cuando al número y la complejidad, y a eso hay que añadirle que los cibercriminales generan un negocio anual estimado de 1,5 billones de dólares. Recientemente leía que el 86% de las empresas espera ser atacadas.



Roberto Alonso
Cloud & Business Director ***GTI***

Si a toda esta combinación le añadimos la llegada del *cloud* a nuestras empresas, los diferentes *endpoints*, la movilidad, la desaparición de un perímetro controlado, el dispositivo particular en el mundo empresarial... es fácil concluir que la CIBERSEGURIDAD es una prioridad de todos.

Desde GTI vemos como parte de nuestra labor catalizar y potenciar las diferentes soluciones que permitan prevenir y remediar el cibercrimen. Y en ese sentido, junto a nuestro tejido de *partners* estamos trabajando en dos vías:

• **Modern Workplace**. Una iniciativa que responde a la evolución del *endpoint* y la gran importancia de estar protegido. Ahora trabajamos con *cloud* públicas, privadas, desde diferentes dispositivos, con diferentes proveedores, con información sensible en múltiples lugares... Simplemente la pérdida o robo de las credenciales puede originar un gran problema. Además, en este entorno no solo miramos la seguridad como tal, sino que trabajamos también en los datos que, definitivamente, tenemos que ser capaces de proteger y gestionar.

Si bien es cierto que, aunque la concienciación cada vez es mayor, quién no tiene un familiar que le ha preguntado por algún problema de este tipo, los riesgos son mayores. Pensemos también en el segmento de mercado de la pyme, donde muchas veces la información crítica reside en un portátil. Protección y recuperación de datos son servicios cada vez más demandados

El canal es clave en el despliegue, ejecución y soporte.

• **Servicios de seguridad gestionados.** En un mercado donde todo nos gusta consumirlo como servicio, la seguridad no podía ser una excepción. Se trata de un modelo de negocio que permite al canal ser más especializado y aterrizar propuestas de negocio diferenciadoras, donde el componente de propiedad intelectual de las soluciones es importante. Además, vemos que se montan servicios avanzados con precios que permiten entrar a empresas de cualquier tamaño, democratizando las soluciones.

Desde GTI vemos la ciberseguridad como un área crítica y de crecimiento para los próximos años. Por eso estamos invirtiendo junto a nuestros *partners* cubriendo todas las necesidades, desde la formación, preventa, soporte, licenciamiento y financiación hasta la generación de negocio. Estamos encantados de acompañar a todos aquellos *dealers* interesados en esta carrera contra el cibercrimen.

Para más asesoramiento en materia de ciberseguridad: **ciber@gti.es**

meras que lo han desarrollado han sido las marcas. "Casi todas están ya en el *cloud*", recuerda. A su juicio, ni se va a estancar el crecimiento ni tiene fecha de caducidad. "Cada día hay más amenazas y, por tanto, más oportunidad". Eso sí, la evolución es de obligado cumplimiento. "O cambiamos y nos reinventamos, o tendremos dificultades para seguir creciendo".

No hay duda de que esta presión sobre los márgenes dificulta la labor del mayorista. "Es más complicado aportar valor al canal", reconoce Chuck Cohen. "Debemos enseñar el camino a los *partners* y evolucionar hacia los modelos de valor añadido que sean compatibles con este entorno".

Siempre cabe la posibilidad de que el mercado evolucione hacia un entorno en el que se incremente la consolidación, que ya se ha producido tanto en el ámbito de las marcas como en el canal. Una situación que convivirá con nuevas incursiones de compañías neófitas en el segmento de la distribución. "Si eres un distribuidor que tiene necesidad de crecer y observas cómo el mercado de la seguridad crece a doble dígito año sobre año es lógico que se plantee una línea de negocio como la seguridad", explica Roberto Alonso. "Será el mercado quien regule quiénes son las buenas y quiénes no". Lo que no cambia un ápice son los servicios. "Siempre han estado detrás de la seguridad", recuerda Enrique Gómez que insiste en que ante tanta competencia es más critico diferenciarse. "Los distribuidores han tomando más conciencia de su necesidad".

Catalizador y orquestador

Ante la enorme fragmentación del mercado, con múltiples soluciones y proveedores, la política que cada mayorista debe seguir para definir su oferta no es tarea sencilla. "Es nuestro gran reto", reconoce Carmen Muñoz. "Ofrecer un portafolio que se pueda gestionar", completa. Además de su valor tecnológico, se observa la capacidad de integración entre las diferentes soluciones, con la capacidad de hacer *cross selling* entre las marcas. "La decisión tecnológica tiene mucho peso", insiste la máxima responsable de Exclusive Group Iberia. "Vemos qué solución falta en la oferta; no qué marca; y en base a ello analizamos qué puede encajar".

"Ser un catalizador es la madre de la ciencia del mayorista y hacerlo de manera correcta, cuando cuentas con un abanico de proveedores, supone poner en marcha muchas iniciativas", corrobora Roberto Alonso. "Hay que saber bien lo que ofreces". En el caso de GTI, una de las oportunidades más claras que han detectado gira en torno a la transformación del puesto de trabajo. "Office365 es el perfecto caballo de Troya en este entorno, que permite al canal vender soluciones de seguridad", señala. Un propósito que requiere reclutar y formar al canal. "En el entorno de los proveedores de servicio tratamos de proporcionarles conocimiento tecnológico, que es un elemento crítico para ellos".

Jorge Puerta,
director comercial de **Ingecom**

"El clásico negocio del antivirus estaba oxidado; sin embargo, las amenazas que tienen como objetivo el puesto de trabajo y, por ende, las tecnologías que se utilizan para detenerlas, han dado un empuje a este entorno, con soluciones que van mucho más allá del antivirus"

A la hora de definir una oferta y, sobre todo, en la tarea de orientar al canal, ¿prima la búsqueda de fabricantes especializados en cada área a proteger o bien se prioriza la instalación de proveedores con una oferta global? Jorge Puerta apuesta por la diversidad. "La seguridad es un ámbito tan grande que no hay un proveedor que sea capaz de abarcarlo todo", explica. "Nadie confiaría la seguridad de la empresa a una sola compañía: es bueno optar por diferentes especialistas en cada una de las áreas (red, puesto de trabajo, redes *wifi*). La riqueza está en la diversidad".

En esta decisión entran en juego los recursos, la capacidad tecnológica para administrar determinadas soluciones y el objetivo de cada compañía (dónde quieren estar y qué áreas del mercado quieren cubrir). "Las marcas tienen, cada vez,

Tech Data
Advanced Solutions

END POINT

Protección de dispositivos e interactuación con los datos y aplicaciones corporativas.

- IoT sensores
- Dispositivos móviles
- Puesto de trabajo
- Servidores

BlackBerry vmware Malwarebytes RSA
cisco Partner IBM STORMSHIELD McAfee

SEGURIDAD DE APLICACIONES

Securización de :

- Desarrollos propios
- Estándar apps
- Descargas

VERACODE

IDENTIDAD Y ACCESO

Control seguro del acceso a servicios y aplicaciones.

- IoT dispositivos
- Movilidad
- Puesto de trabajo
- Aplicaciones /SaaS

RSA SONICWALL ONE IDENTITY cisco Partner

SEGURIDAD AUTOMATIZADA Y MONITORIZACIÓN

- Vigilancia
- Respuesta frente a ataques
- Detección de amenazas persistentes

STORMSHIELD McAfee RSA

CONTENIDOS

Securización frente a amenazas del contenido.

- BBDD, Big Data, BI, Analytics
- Storage y Back up
- Buzones de correo
- Servidores de ficheros

SONICWALL McAfee STORMSHIELD cisco Partner

SEGURIDAD EN LA RED

Protección perimetral y acceso seguro frente a amenazas.

- Control de acceso
- End to end encryption
- NGF / Firewall
- WAF, DoS, Proxi, Mail
- IPS /IDS

RSA SONICWALL STORMSHIELD cisco Partner radware
IBM McAfee

Contacta con Tech Data

más presencia en los mercados locales, por lo que la decisión no es solo tecnológica sino observar dónde hay oportunidades y analizar si puede ser, o no, un *partner* predominante para una marca. Es una decisión de negocio importante", explica Carmen Muñoz.

Antonio Anchustegui recomienda equilibrar esta diversidad con la necesaria administración. "Si una empresa tiene recursos limitados es mejor que apueste por un solo proveedor o por unos pocos que le permitan cubrir su seguridad de manera fiable". El responsable de seguridad de Ingram Micro explica que tan importante es el diseño e instalación de las soluciones, como la aplicación de buenas prácticas y políticas adecuadas en materia de seguridad. "Deben existir profesionales que se encarguen del establecimiento y administración de las políticas de seguridad: actualización, cifrado, etc.".

El canal mayorista y, por ende, el distribuidor ha venido trabajando en un modo "silo" con un desarrollo, particular, de cada marca. "Hay que intensificar la apuesta por la construcción de soluciones a partir de la combinación de varios fabricantes, a las que se puede sumar una capa de servicios (formación, financiación, etc.)", recuerda Iñaki López. Una filosofía que permitirá hacer único a cada mayorista o a cada distribuidor, lo que aliviará la competencia. "Cada uno de los miembros del canal tendrá una oferta concreta, empaquetada de una manera diferente, que irá dirigida a un nicho de mercado; lo que reportará un retorno de la inversión mayor al que estamos teniendo", explica. Se trata, en definitiva, de trabajar más la propia marca. "Hay que construir soluciones que nos hagan únicos".

Chuck Cohen,
fundador y director general de **Ireo**

"Debemos enseñar el camino a los *partners* y evolucionar hacia los modelos de valor añadido que les permitan elevar sus márgenes"

bilidad", explica Chuck Cohen. "Otros, sin embargo, con perfiles más especializados, optan por soluciones de nicho, con más profundidad, lo que les permite añadir valor", continúa.

El *ransomware* ha sufrido una rápida transformación en los últimos tres años, mejorando la arquitectura del *malware* para aumentar su precisión y las técnicas para acceder a las *botnets*

Ayudar al canal a encontrar su propia oferta es, por tanto, la clave. "La tecnología es importante, debe ser de primer nivel; pero una vez que ya se está jugando en el primer nivel, la guerra tecnológica es un ámbito que pertenece a las marcas", explica Enrique Gómez. "No es la nuestra", insiste; "la nuestra es el negocio del canal: cuidar y formar al *partner* para que encuentre la rentabilidad del negocio".

La diversidad de perfiles que exhibe el canal no facilita la labor al mayorista que debe cubrir a todos. "Algunos socios prefieren una solución más fácil de vender, que cumpla con los requerimientos del cliente, generando una buena rentabilidad", explica Chuck Cohen. "Otros, sin embargo, con perfiles más especializados, optan por soluciones de nicho, con más profundidad, lo que les permite añadir valor", continúa. "Nuestra labor es dar cobertura a todo el espectro, lo que la concede más complicación".

Tampoco es sencillo enarbolar el carácter único que deben tener todas y cada una de las compañías que forman parte del canal. Las marcas no lo ponen sencillo: su crecimiento las conduce en la mayoría de los casos a tomar la decisión de ampliar su canal para alcanzar una mayor cobertura. "Cuando un fabricante triunfa, generalmente firma con más distribuidores y el margen se reduce", recuerda Iñaki López. Es fundamental, entonces, "analizar la manera de ser únicos y cómo proteger nuestra propiedad intelectual".

Protegiendo el elemento humano; el ataque a infraestructuras es cosa del pasado

La nueva era de dispositivos conectados (IoT) ha propiciado que los hackers hayan desarrollado nuevas fórmulas de ataque mucho más precisas, así como nuevos "objetivos" contra los que impactar. Cualquier dispositivo conectado está en riesgo. Asimismo, y a medida que las aplicaciones empresariales migran a la nube, también lo hacen las amenazas, sorteando la seguridad del perímetro corporativo.

Sin embargo, y pese a la evolución de las amenazas, centradas hoy más que nunca en el robo de datos confidenciales, hay una cosa que no cambia: el factor humano. Según el estudio Human Factor 2018 elaborado por Proofpoint, empresa de ciberseguridad de nueva generación, los ciberdelincuentes prefieren explotar los instintos de curiosidad y confianza humanos en lugar de basarse en vulnerabilidades de software y hardware. De hecho, más del 93 % de los ataques dirigidos se activa por medio de los usuarios, ya sea haciendo clic en un enlace malicioso, escribiendo una contraseña en una web de *phishing* o enviando datos confidenciales tras recibir un *email* fraudulento.

A este respecto, es llamativo que, pese a esta realidad, las organizaciones solo destinen un pequeño porcentaje (8 %) de su inversión en seguridad a proteger el correo electrónico, el vector más utilizado por los cibercriminales, en vez de invertir en soluciones tecnológicas que ayuden a detener las amenazas dirigidas, salvaguardar los datos y a hacer a los usuarios más resilientes frente a ciberataques.

La mejor defensa es un buen ataque

En las organizaciones modernas, los empleados, los datos y los dispositivos pueden estar en cualquier parte. Para defender los activos empresariales, las defensas de hoy deben funcionar en todas partes, lo que brinda un mayor contexto para analizar y extraer inteligencia sobre amenazas, reducir la superficie de ataque y disminuir el riesgo de asalto. Los daños y efectos producidos por estas amenazas pueden causar un impacto devastador en los sistemas de información empresariales, con pérdida permanente de datos críticos para éstas.

proofpoint™

Como mayorista especializado en ciberseguridad y cloud, Exclusive Networks recomienda la integración de una solución de seguridad de nueva generación, como Proofpoint, eficaz para la protección de los usuarios, los datos y las marcas de ataques avanzados y riesgos de cumplimiento.

Proofpoint cuenta con una tecnología capaz de detener las amenazas avanzadas, incluyendo *ransomware* y otras variantes distribuidas a través de adjuntos y URLs, amenazas de día cero, *malware* polifórmico o *phishing*, antes de que lleguen a los usuarios. Proofpoint también detecta las amenazas y los riesgos para las aplicaciones en la nube, relacionadas con ataques por correo electrónico cuyo objetivo es el robo de credenciales o de otro tipo; protege la información creada por las personas, para reducir la exposición a ataques y el riesgo de cumplimiento; y permite a los usuarios responder rápidamente cuando las cosas no están bien.

Aunque las tecnologías que pueden detectar y bloquear los mensajes maliciosos son parte de la solución de Proofpoint, no hay que olvidar que más del 90 % de los ciberataques comienzan por un mensaje de correo electrónico. Para reducir las probabilidades de éxito de los ataques de *phishing* o *ransomware*, Proofpoint cuenta con la plataforma Security Awareness Training, una potente herramienta de evaluación del conocimiento basada en la web que identifica las posibles vulnerabilidades de los empleados, mediante técnicas de ataque simulado. Proofpoint puede proporcionar a sus clientes toda la información que necesitan para identificar y proteger a sus individuos más expuestos a ciberataques. Sin embargo, en ningún caso, debe prescindirse del sentido común. La naturaleza humana es inconstante, por lo que ninguna fuerza laboral, ni siquiera la más joven, lleva aparejada una conciencia innata de las amenazas a la ciberseguridad.

EXCLUSIVE NETWORKS

"El mercado de la ciberseguridad continúa creciendo y esto se ha visto reflejado en nuestros resultados"

El año pasado, Ingecom cerró ejercicio fiscal alcanzando los 24,8 millones de euros de facturación, registrando un crecimiento cercano al 10 % con respecto al ejercicio precedente. ¿Cómo se está presentando este 2019?

En general, el mercado de IT se está ralentizando debido en gran parte a la incertidumbre política del país. Esto mismo ocurre a nivel global en el ámbito económico. A pesar de esta tendencia del mercado, este primer trimestre hemos incrementado la facturación gracias, a que dentro del sector IT, la parte de ciberseguridad se mantiene a buen ritmo de crecimiento. Esto se ha visto reflejado en nuestros resultados a cierre de trimestre, donde esperamos alcanzar los 9 millones de euros de facturación, lo que supone un crecimiento elevado frente al mismo período del año pasado.

Recientemente han anunciado la apertura de una oficina física en Italia, ¿qué retos se han marcado a corto plazo en este país?

Desembarcamos en Italia en febrero con la apertura de una oficina física en Milán. En el país transalpino hemos empezado con parte del *portfolio* que tenemos en Iberia que incluye a fabricantes como Array Networks, Cymulate, Hdiv Security, SealPath, Thycotic, Viewtinet y WhiteBearSolutions. Todos ellos los distribuiremos en exclusividad en el mercado italiano, con el fin de ayudar a los fabricantes a crecer en este territorio. Sergio Manidi está al frente de Ingecom Italia como country manager desde hace dos meses, un profesional con amplia experiencia en el canal italiano y, sobre todo, en el canal especializado.

Javier Modúbar,
*CEO de **Ingecom**, mayorista de valor especializado en soluciones de seguridad IT y ciberseguridad*

En 2018 una buena parte de las estrategias de seguridad de las empresas giraba en torno a GDPR. Desde su punto de vista, este año, ¿cuáles son las propuestas de seguridad que están actuando como dinamizadoras del sector de la ciberseguridad?

Las tendencias del mercado en ciberseguridad se basan en proteger el puesto de trabajo, el dato y al ser humano, por lo que veremos bastantes proyectos basados en tecnología PAM, IRM, DLP, UEBA o NAC. En este sentido, es importante dotarse de herramientas de detección de vulnerabilidades y de simulación de ataques para comprobar si la inversión realizada en seguridad cubre la mayor parte de las amenazas que pueden darse en una organización. A esto se le añade que los entornos industriales son cada vez más un foco de ataques, por lo que veremos una fusión entre IT y OT.

¿Qué puede aportar Ingecom a ese entorno OT (Tecnología Operacional)?

Esta fusión IT y OT demandará herramientas de monitorización y prevención tradicionales del mundo IT para abarcar la seguridad OT. Ingecom ha firmado un acuerdo de distribución con Indegy, al mismo tiempo que nuestro fabricante Forescout ha comprado SecurityMatters con el fin de abordar este mundo desde diferentes enfoques.

"Las tendencias del mercado en ciberseguridad se basan en proteger el puesto de trabajo, el dato y al ser humano, por lo que veremos bastantes proyectos basados en tecnología PAM, IRM, DLP, UEBA o NAC"